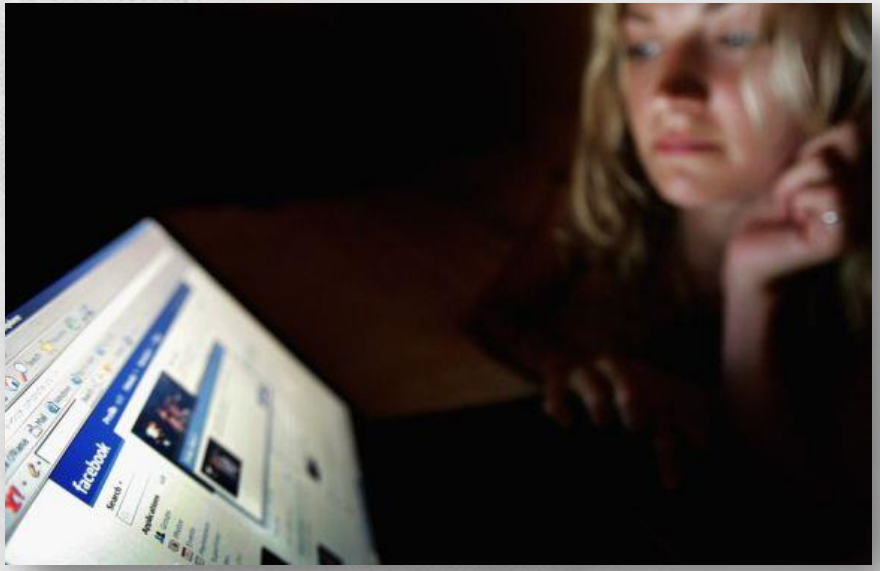

CHANGING
TRENDS

THE BIRTH OF
THE TECHNOLOGICAL SOCIETY

BEFORE WE DISCUSS NEW TRENDS IN INTERNET BLACK HAT HACKING, WE SHOULD PROVIDE SOME ANSWERS ABOUT THE CURRENT, SECURITY-COMPROMISING CHANGES IN USERS' BEHAVIOUR

The new developments in technology have completely reshaped how people are communicating in the twenty-first century

THE BIRTH OF
THE TECHNOLOGICAL SOCIETY



IF FACEBOOK WERE A COUNTRY, with over a billion users it would be the third most-populated in the world, just behind China and India

THE BIRTH OF
THE TECHNOLOGICAL SOCIETY

THIS COMMUNICATION UPHEAVAL HAS LEAD TO RE-DEFINING THE WORD FRIEND.

A friend is a person you don't know personally but who has the same interests as you. You don't necessarily trust your online friends

THE BIRTH OF
THE TECHNOLOGICAL SOCIETY

WE PUBLISH MORE AND MORE PERSONAL INFORMATION ONLINE

which leads to privacy issues. When you put up something online, you lose control over it and don't know how it will be used by others.

THE BIRTH OF
THE TECHNOLOGICAL SOCIETY

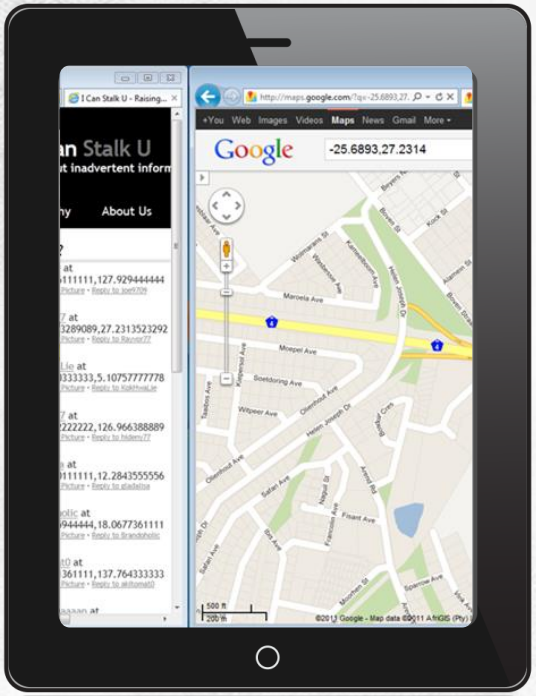
AN ATTACKER EXPLOITS THIS CHANGE IN TWO WAYS:

By collecting information about you

By impersonating others to gain your trust

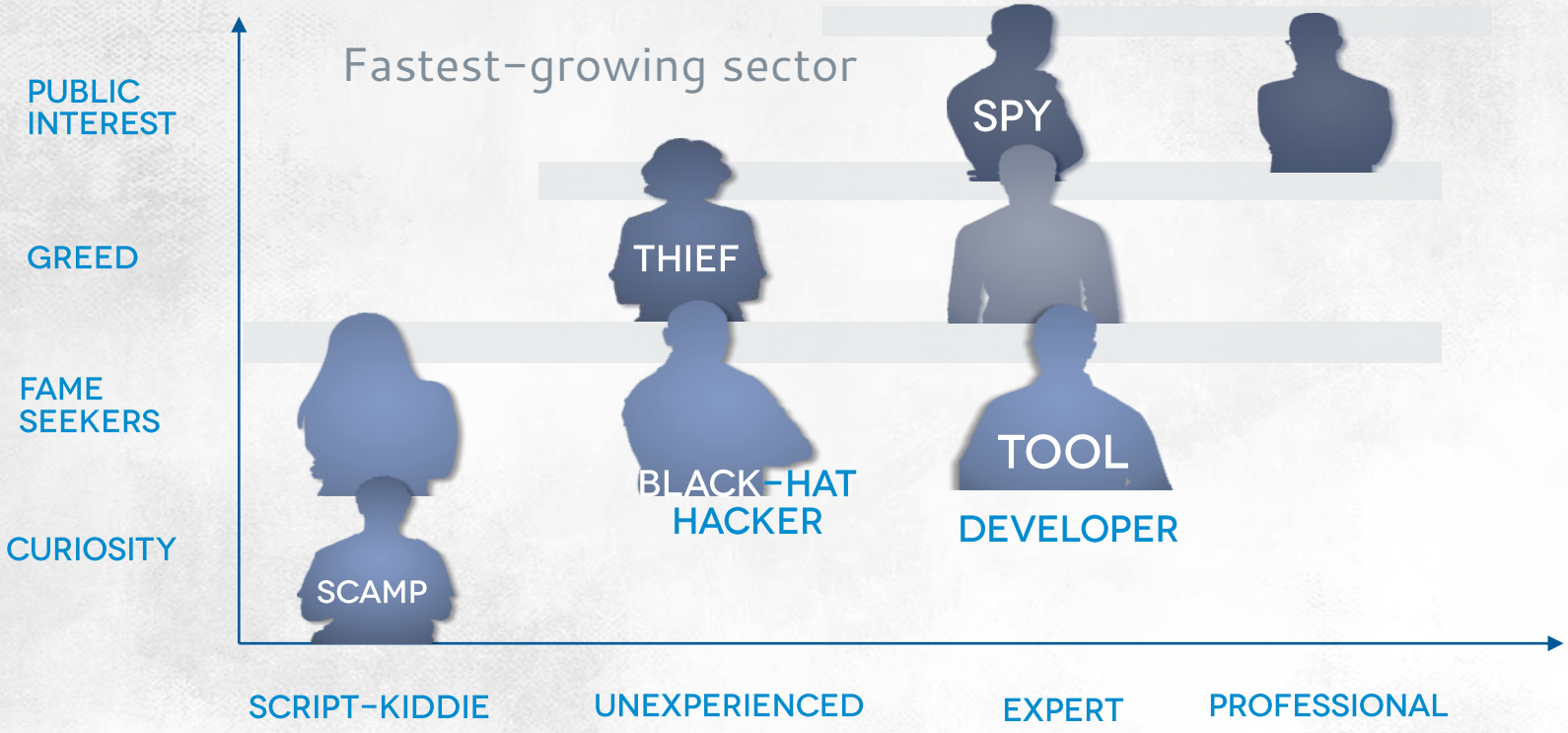
EXERCISE HOW MUCH INFO

about you is on the Internet?



- **PUBLIC RECORDS AGGREGATES**
  www.findmypast.com
  www.intelius.com
- **SOCIAL NETWORKING SITES SEARCHES**
  www.kgbpeople.com
  www.spokeo.com
- **POSTING PHOTOS TAGGED WITH DATE AND LOCATION**
  www.icanstalku.com
- **PRIVACY-BREACHING SERVICES**
  www.readnotify.com
  www.mylife.com
- **SPECIALIZED APPLICATIONS**
  Maltego
- **ONLINE FRIENDS**
  facebook blaster pro

CYBER CRIMINALS



THE BOA FACTOR

SET UP IN THE 90S, BOAFACTORY.COM WAS
a website that offered credit card numbers for sale at a good price

THE BOA FACTOR

THE BOA FACTORY PEOPLE HAVE STOLEN 154,000 CREDIT CARD DETAILS FROM AMONG OTHERS:

- Marriott Hotels
- Rich Solutions
- DPI
- SLM Soft
- Global Card Services
- Isabel Bloom
- IMAX
- Tempe AZ
- Innobeta ATM network

Arrested and deported to the USA, BOA was charged with fraudulently obtaining 2.5 million dollars.

HE WAS ALSO LIKELY INVOLVED IN A CYPRUS-REGISTERED OFFSHORE COMPANY THAT LAUNDERED 200 MILLIONS.

THE BOA FACTOR

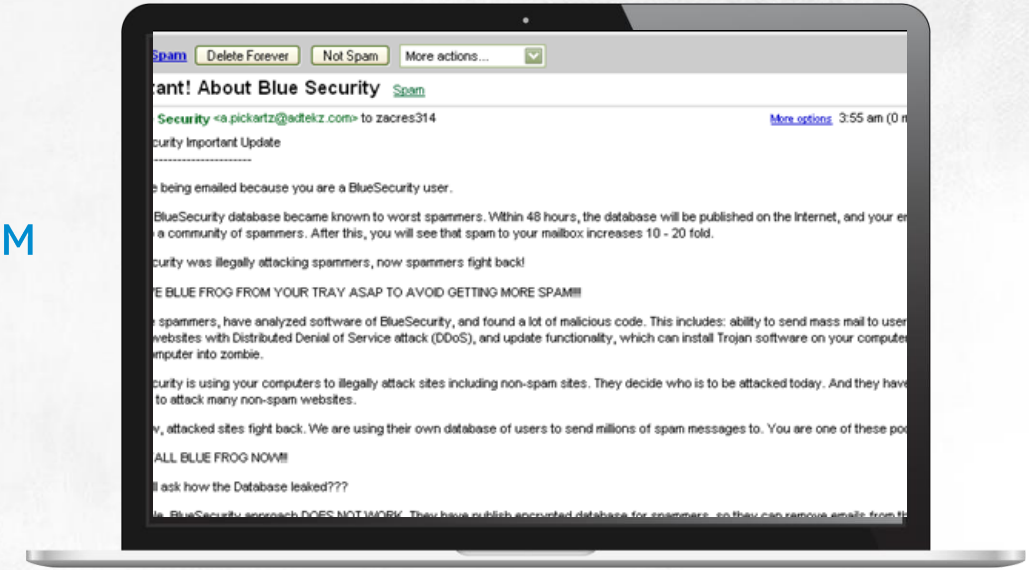
IGOR ANATOLY
TERESCHENKO

BOA, ROMAN VEGA,
ROMEO ANTONIO VEGA,
MIKE OLDFIELD,JERRY DEEWOOD

BLUE SECURITY ATTACKED

IN 2005 BLUE SECURITY LAUNCHED ITS FLAGSHIP PRODUCT, THE GROUND-BREAKING ANTI-SPAM SYSTEM BLUE FROG.

It was so good it jeopardized the operation of the Russian company PharmaMaster, a fake Viagra seller.



BLUE SECURITY ATTACKED

On May 01 2006 spammers targeted Blue Frog users, sending them emails with threats

Simultaneously, Blue Security servers were attacked: first foreign access was blocked, next a DDoS attack caused all the servers to fold.

The company transferred its website to an external provider's servers (Prolexic). After a week, also this company's and their clients' servers (more than 2,000 in total) were blocked due to the attack

ON MAY 17, BLUE SECURITY FOLDED AND WITHDREW BLUE FROG

BLA BLA

OVER JUST THREE YEARS (2005 to 2007) Albert Gonzalez managed to sniff out 170 million credit card details

GONZALEZ ASKED HIS PAL Stephen Watt, a software developer in Morgan Stanley to create a web scanner called Blabla

UNDETECTED BY ANTI-VIRUSES and IDS systems, the program broke into the TJX corporation network in 2005 and sniffed out over 45 million credit card details

BLA BLA

OVER THE NEXT TWO YEARS,
Gonzalez used this scheme to break into the Heartland Payment Systems, Hannaford Brothers and Citibank ATM system networks

STEPHEN WATT PLEAD GUILTY AND WAS SENTENCED TO TWO YEARS IN PRISON AND FINED WITH PAYING 170 MILLION DOLLARS IN RETRIBUTION. GONZALEZ IS STILL SERVING HIS 15- TO 25-YEAR PRISON SENTENCE. ON RELEASE, HE WILL PAY 70 MILLION DOLLARS.

CHINESE PENIS-ENLARGEMENT PILLS AD

IN JANUARY 2007 A MASS-MAILING VIRUS
called Storm Worm was detected. The virus launched a Trojan horse in the victim computer after a user would open an email attachment. The computer was then added to a zombie net.

By September, the attacker-controlled botnet counted as many as 10 million hosts

CHINESE PENIS-ENLARGEMENT PILLS AD

Infected computers sent out 900 million Chinese penis-enlargement pill ads daily

The income from clicking ad banners on the websites was 7 thousand dollars daily

If a company deemed the penis-enlargement ads as spam, the Storm Worm-infected computer would attack this company's servers

CYBERWAR

THE FIRST CYBERWAR BROKE IN 2007 WHEN CHINA ATTACKED

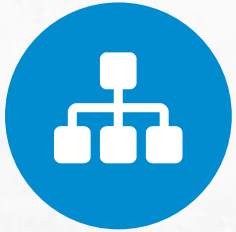
Germany and the US. Soon after this, Estonia became a target of another wave of cyberattacks

CYBERWAR

CYBERWARS WILL EMERGE AS A MORE AND MORE PREVALENT REALITY:

The global computer network is extremely vulnerable to attacks.

Attacking computer systems is much easier and cheaper than protecting them effectively



You don't need a lot to launch a cyberattack

It's hard to discover attackers fighting a cyberwar, whether it's still being planned or already in progress

CYBERWAR

CYBERWARS WILL EMERGE AS A MORE AND MORE PREVALENT REALITY:

Countries lack adequate protective measures

Detecting the culprits of other attacks is much easier then detecting the culprits of a cyberattack

CYBERWAR

CYBERWARS WILL EMERGE AS A MORE AND MORE PREVALENT REALITY:

THE GOALS OF CYBERWARS:

- Espionage
- Propaganda
- Shutting down nation-critical services

CYBERWAR

CYBERWARS WILL EMERGE AS A MORE AND MORE PREVALENT REALITY:

What could happen if there was no Internet for a day, a week or a month?

- No emails
- No social networking sites
- Inactive smartphones
- No e-commerce

And what if specialist computer systems were blocked for a day, a week or a month?

- Airports and stations shut down
- No electricity
- No water supply
- Institutions closed

CYBERWAR

ESTONIA

THE FIRST WEB WAR (2007) STARTED

around the time when a monument commemorating Soviet soldiers, the Bronze Soldier of Tallinn, was removed from the centre of Estonia's capital city

CYBERWAR

ESTONIA

FOR THREE WEEKS, ESTONIA WAS PARALYZED
with 130 different distributed denial of service (DDoS) attacks launched against the country's parliament, banks, government departments, news agencies and governmental websites. Also the Estonian embassy in Russia suffered from the attacks

DESPITE THE LACK OF EVIDENCE LINKING THE KREMLIN
to the attack, it's commonly agreed that Russian hackers alone would not be able to plan and run such a large-scale operation

CYBERWAR

GEORGIA

IN 2008 AN ARMY OF ATTACKERS HAILING FROM RUSSIA COMPLETELY SHUT DOWN GEORGIA'S INTERNET SERVICES

The attacks were concurrent with Russian military forces invading Georgia

Because of the blockage, both the authorities and the public were unable to follow the military operations

CYBERWAR

GEORGIA

11 GOVERNMENTAL WEBSITES were targeted and cut off using botnets that redirected Torrent network traffic to the websites.

Other botnets blocked 43 websites of various news agencies

CYBERWAR

GOOGLE

IN 2010 GOOGLE DISCOVERED

and publicised a highly-sophisticated attack that targeted Chinese activists and European and American citizens

HUMAN RIGHTS

activists was spyed on by malware that was installed on their computers to check on and control their email boxes

CYBERWAR

GOOGLE

INVESTIGATION REVEALED THAT

the attack was launched a year before from hosts located in China. Apart from dissidents, it targeted many American hi-tech, chemical, industrial, financial and mass media companies. The objective was to steal confidential information stored on the computers

CYBERWAR

STUXNET WORM

IN JUNE 2010 NEWS BROKE OF FIRST VIRUS THAT EXPLOITED HIGHLY SPECIALIST TECHNOLOGY AND HID IN PLC DEVICES USING A CUSTOM ROOTKIT

The virus was used to launch a cyberattack on Iranian uranium enrichment plants. For the first fifteen minutes it accelerated the speed of centrifuges used for cooling nuclear fuel by 30%, and after 27 days it would decelerate the speed for 40 minutes by 50%

CYBERWAR

STUXNET WORM

BEFORE IT WAS CAUGHT AND REMOVED, IT FORCED THE REPLACEMENT OF EVEN A THOUSAND CENTRIFUGES

STUNNINGLY SOPHISTICATED, THIS ATTACK COULD NOT HAVE BEEN LAUNCHED WITHOUT GOVERNMENTAL HELP

Stuxnet Worm spread through USB flash drives and networks. Once launched, it attacked Windows systems by using four different zero-day security vulnerabilities. The virus signature was fake, using a stolen certificate issued by a trusted certificate authority

RECAP

FAME

MASS DESTRUCTION

MEDIA COVERAGE

IMPERSONATING

SPYWARE

TARGETED ATTACKS

PROFITABLE

THANKS